II. SPECIFICATION AMENDMENTS

On page 1, after the title, please insert the heading:

- - BACKGROUND OF THE INVENTION - -

B1

On page 1, before line 4, please insert the heading:

- - 1. Field of the Invention - -

Please delete the paragraph beginning on page 1, line 4 through line 7, and replace it as rewritten below:

B2

-- The present invention generally relates to a mobile station in a mobile network, and in particular to authenticating a mobile station in a mobile network. --

On page 1, between lines 7 and 8, please insert the heading:

B3

- - 2. Brief Description of Related Developments - -

Please replace the paragraph beginning on page 1, line 8 through line 16 as rewritten below:

Known authentication and key agreement protocols are based either on symmetric or public key cryptography and a trusted third party. In ~~GSM~~a Global System for Mobile Communication ("GSM"), the authentication and encryption key agreement is based on symmetric key and a trusted third party. The method using symmetric key requires the existence of an agreed secret between communicating parties or with a server as the third party. In GSM the mobile station of the subscriber shares a secret subscriber

authentication key K_i with a trusted authentication centre AC. The authentication of the mobile station is based on the use of a one-way function A3 and a ciphering key K_c is derived from the shared K_i in the mobile station and the authentication centre.

Please replace the paragraph on page 3, line 16 through line 20, as rewritten below:

~~What is characterizing to the method according to the invention is presented in claim 1. What is characterizing to the communications system of the invention is presented in claim 9. What is characterizing to the mobile station of the invention is present in claim 11. Preferable embodiments of the invention are described in the dependent claims.~~

In one aspect, the present is directed to authenticating a mobile station in a mobile network. In one embodiment the method includes authenticating the mobile station with user-to-user data exchange.

In another aspect, the present invention is directed to a cellular communications system including a first mobile station, a second mobile station and at least one mobile switching centre. In one embodiment the first and second mobile stations are wirelessly connected via base stations. The first mobile station constructs and sends a first message and receives and verifies the validity of a second message. When the information is verified as valid, the first mobile station accepts to share a shared encryption key K, and constructs and sends a third message. A second mobile station receives the first message and constructs and sends the second message. The second mobile station receives and verifies the validity of the third message, and when the information is determined to be valid, accepts to share the shared encryption key K with the first mobile station.

In a further aspect the present invention is directed to a mobile station. In one embodiment the mobile station includes a processor, a memory, an output means, an input means, a transmitter/receiver and an antenna. The processor performs operations needed to form and verify messages and implements authentication and key agreement procedures. The procedures and messages, with necessary parameters and variables, are stored in the memory. The commencement of extra secure communications is presented to a user of the mobile station via the output means. The input means is used to enable validation of the extra secure communication and the transmitter/receiver and antenna transform information to radio waves from digital signals and vice versa.

B4

On page 3, between lines 20 and 21, please insert the heading:

- - SUMMARY OF THE INVENTION - -

Please replace the paragraph on page 3, line 21 through line 23, as rewritten below:

The invention ~~concerns~~is directed to a method to authenticate a mobile station in a mobile network. According to the invention the mobile station is authenticated using user-to-user data exchange. This can be done during call setup or call.

Please replace the paragraph on page 3, line 26 through page 4, line 5 as rewritten below:

B5

The invention ~~concerns also~~is also directed to a cellular communications system, where the first and second mobile stations

(A, B) are connected wireless with via base stations. According to the invention the cellular communications system comprises a first mobile station (A), that constructs and sends a first message (M_1), receives and verifies the validity of a second message (M_2) and when the information is verified valid accepts to share a shared encryption key K, constructs and sends a third message (M_3), a second mobile station (B), that receives the first message (M_1) and constructs and sends the second message (M_2), receives and verifies the validity of the third message (M_3) and when the information is valid accepts to share the shared encryption key K with the first mobile station (A), and at least one mobile switching centre.

Please replace the paragraph on page 4, line 6 through line 13 as rewritten below:

The invention ~~concerns also~~is also directed to a mobile station. According to the invention the mobile station comprises a processor to perform operations needed to form and verify messages (M_1, M_2, M_3), to implement authentication and key agreement procedures, a memory, where procedures and messages are stored with necessary parameters and variables, output means, on which commencement of extra secure communication is presented to a user of the mobile station, input means to enable validation of the extra secure communication, a transmitter/receiver and an antenna to transform information to radio waves from digital signals and vice versa.

On page 4, between lines 16 and 17, please insert the heading:

-- BRIEF DESCRIPTION OF THE DRAWINGS --

On page 4, between lines 25 and 26, please insert the heading:

B7

-- DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(s)--

On page 9, after line 24, please insert the following:

-- What is claimed is: --